Microsoften segurtasun eguneraketa – 2021ko urria

BCSC-EGUNERAKETA-MICROSOFT-2021-URRIA

TLP:WHITE

www.basquecybersecurity.eus

2021eko urria

AURKIBIDEA

Erantzukizunetik salbuesteari buruzko klausula

Honako dokumentu hau eskaintzen da erakundeen eta interesa duten herritarren segurtasunerako BCSCk beharrezkotzat jotzen dituen alertak ezagutzera emateko. Inongo kasutan BCSC ezin da kontsideratu hemen zabaldutako informazioaren erabilpenak zuzenean nahiz zeharka, ustekabean nahiz modu berezian, eragin litzakeen balizko kalteen arduradun. Gauza bera esan beharra dago BCSCren webean edo hortik esteken bitartez joan litekeen kanpoko web orrialdeetan, sare sozialetan, software produktuetan edo alertan nahiz BCSCren webean agertutako beste edozein informaziotan aipa litezkeen teknologiei dagokienez. Edozein kasutan, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak hemen jasotako terminoetan emandako iritzi eta gomendioak dira eta jakinarazitako informaziotik ezin da ondorioztatu ondorio juridiko loteslerik.

Salmenta debekatzeari buruzko klausula

BCSC-RI BURUZ

Zibersegurtasun Euskal Zentroa (Basque Cybersecurity Centre, BCSC) da Eusko Jaurlaritzak izendatutako entitatea Euskadin zibersegurtasunaren gaian heldutasun maila igotzeko.

Zeharkako ekimena da, Enpresa Garapenerako Euskal Agentziaren (SPRI) barnean kokatua, Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren menpe dagoen sozietatea. Era berean, Eusko Jaurlaritzako beste hiru Sail ere bere parte dira: Segurtasuna, Gobernantza Publiko eta Autogobernua, eta Hezkuntza; bai eta Zientzia, Teknologia eta Berrikuntzako Euskal Sistemako lau eragile ere: Tecnalia, Vicomtech, Ikerlan eta BCAM.

BCSC erreferentziazko entitatea da zibersegurtasuna eta konfiantza digitala garatzeko Euskadiko herritar, enpresa eta instituzio publikoen artean, eta batez ere, eskualdeko ekonomiaren sektore estrategikoen kasuan.

Beraz, BCSCren eginkizuna da euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa jarduera dinamizatzea, eta erreferentzia izango den sektore profesional bat sor dadin eragitea. Testuinguru horretan osagarriak diren eragileen arteko lankidetza proiektuak exekutatzea sustatzen du, berrikuntza teknologikoaren, ikerkuntzaren, eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren alorretan.

Era berean, hainbat zerbitzu eskaintzen ditu Gertakarien Aurreko Ekipo modura duen rolagatik (aurrerantzean CERT, ingeleseko izenaren siglak direla-eta “Computer Emergency Response Team”). Euskal Autonomia Erkidegoko esparruan mehatxu berriak antzemateko eta horiei buruzko alerta goiztiarrak emateko gaitasuna areagotzen dihardu lanean, informazioaren segurtasun gertakarien erantzunean eta analisian, eta euskal gizartearen beharrak artatzeko beharrezkoak diren prebentzio neurrien diseinuan. Helburu horiek lortzeko xedearekin, zibersegurtasun gertakariak kudeatzera zuzendutako hainbat ekimenetan hartzen du parte:

1. LABURPEN EXEKUTIBOA

Hileroko bigarren asteartean ohikoa izaten den moduan, Microsoftek 2021eko urriko segurtasun eguneraketak argitaratu ditu.Eguneraketa hauekin 71 ahultasun zuzentzen dira, edo 82, Microsoft Edge-ri eragiten dioten 8 ahultasunak eta OpenSSL-rekin zerikusia duten hirurak kontuan hartzen badira.

Zuzendutako ahultasunetako bat aktiboki baliatua izaten ari zen (CVE-2021-40449) eta horietako hiruri buruz (CVE-2021-41338, CVE-2021-40469, CVE-2021-41335) informazioa argitaratuta zegoen.Larritasunari dagokionez, ahultasunetako 3 kritikotzat joak izan dira, 70 garrantzitsu modura eta 1 baxu modura.

Ahultasunen eragin motari dagokionez:

- Pribilegioen igoera erako 21 ahultasun.
- Segurtasun funtzioen saiheste erako 6 ahultasun.
- Kodearen urruneko exekuzio erako 20 ahultasun.
- Informazioaren hedatze erako 13 ahultasun.
- Zerbitzuaren ukapen erako 5 ahultasun.
- Spoofing erako 9 ahultasun.

Kaltetutako produktuen artean Microsoft Office, Exchange Server, MSHTML, Visual Studio eta Edge nabigatzailea daude, beste batzuen artean.

Ohikoa den moduan, ahultasun hauek eta beste batzuk prebenitzeko BCSCk gomendatzen du gure sistemak eta aplikazioak azken bertsiora eguneratuta izatea beti.

2. KALTETUTAKO BALIABIDEAK

Urriko segurtasun partxeek honako produktu hauei eragiten dieten segurtasun ahultasunekin daukate zerikusia:

- .NET Core & Visual Studio
- Active Directory Federation Services
- Console Window Host
- HTTP.sys
- Microsoft DWM Core Library
- Microsoft Dynamics
- Microsoft Dynamics 365 sales
- Microsoft Edge (Chromium based)
- Microsoft Exchange Server
- Microsoft Graphics Component
- Microsoft Intune
- Microsoft Office Excel
- Microsoft Office SharePoint
- Microsoft Office Visio
- Microsoft Office Word
- Microsoft Windows Codecs Library
- Rich Text Edit Control
- Role: DNS Server
- Role: Windows Active Directory Server
- Role: Windows AD FS Server
- Role: Windows Hyper-V
- System Center
- Visual Studio
- Windows AppContainer
- Windows Appx Deployment Service
- Windows Bind Filter Driver
- Windows Cloud Files Mini FIlter Driver
- Windows Common Log File System Driver
- Windows Desktop Bridge

- Windows DirectX
- Windows Event Tracing
- Windows exFAt file system
- Windows Fastfat Driver
- Windows Installer
- Windows Kernel
- Windows MSHTML Platform
- Windows Nearby Sharing
- Windows Network Address Translation (NAT)
- Windows Print Spooler Components
- Windows Remote Procedure Call Runtime
- Windows Storage Spaces Controller
- Windows TCP/IP
- Windows Text Shaping
- Windows Win32k

3. AZTERKETA TEKNIKOA

Hileroko bigarren asteartean ohikoa izaten den moduan, Microsoftek 2021eko urriko segurtasun eguneraketak argitaratu ditu.Eguneraketa hauekin 71 ahultasun zuzentzen dira, edo 82, Microsoft Edge-ri eragiten dioten 8 ahultasunak eta OpenSSL-rekin zerikusia duten hirurak kontuan hartzen badira.

Zuzendutako ahultasunetako bat aktiboki baliatua izaten ari zen (CVE-2021-40449) eta horietako hiruri buruz (CVE-2021-41338, CVE-2021-40469, CVE-2021-41335) informazioa argitaratuta zegoen.Larritasunari dagokionez, ahultasunetako 3 kritikotzat joak izan dira, 70 garrantzitsu modura eta 1 baxu modura.

Hiru ahultasun kritikoei dagokienez, CVE-2021-40486, CVE-2021-38672 eta CVE-2021-40461, kodearen urruneko exekuzio erako 3 ahultasun dira. Lehenak Microsoft Wordi eragiten dio, eta gainerako biek Hyper-V-ri eragiten diote.

Aktiboki baliatua izaten ari zen ahultasunari dagokionez, CVE-2021-40449 identifikatzailea daukana, Win32k-ren kernelaren driverraren pribilegioen igotze erako ahultasun bat da. Hori baliatuz asmo gaiztoko eragile batek pribilegio altuak eskura litzake Windows gailu batean.

Informazioa argitaratuta zeukaten ahultasunei dagokienez:

- CVE-2021-41338: Windows AppContainer Firewall-en akatsa, erasotzaileei segurtasun funtzioak saihestea ahalbidetzen diena
- CVE-2021-40469: Kodearen urruneko exekuzioa Windowsen DNS zerbitzarian
- CVE-2021-41335: Pribilegioen igotze erako ahultasuna Windowsen kernel-ean.

Identifikatutako ahultasun guztien zerrenda eskaintzen da segidan:

CVE	Izenburua	Larritasuna
CVE-2021-40461	Kodearen urruneko exekuzio erako ahultasuna Windows Hyper-V-n	**Kritikoa**
CVE-2021-38672	Kodearen urruneko exekuzio erako ahultasuna Windows Hyper-V-n	**Kritikoa**
CVE-2021-40486	Kodearen urruneko exekuzio erako ahultasuna Microsoft Worden	**Kritikoa**
CVE-2021-41330	Kodearen urruneko exekuzio erako ahultasuna Microsoft	Garrantzitsua

	Windows Media Foundation-en	
CVE-2021-26442	Pribilegioen igotze erako ahultasuna http.sys windows-en	Garrantzitsua
CVE-2021-26441	Pribilegioen igotze erako ahultasuna storage Spaces Controller-en	Garrantzitsua
CVE-2021-40489	Pribilegioen igotze erako ahultasuna storage Spaces Controller-en	Garrantzitsua
CVE-2021-40488	Pribilegioen igotze erako ahultasuna storage Spaces Controller-en	Garrantzitsua
CVE-2021-40487	Kodearen urruneko exekuzio erako ahultasuna Microsoft SharePoint Server-en	Garrantzitsua
CVE-2021-34453	Zerbitzuaren ukapen erako ahultasuna Microsoft Exchange Server-en	Garrantzitsua
CVE-2021-40485	Kodearen urruneko exekuzio erako ahultasuna Microsoft Excelen	Garrantzitsua
CVE-2021-40484	Ordezpen erako ahultasuna Microsoft Sharepoint server-en	Garrantzitsua
CVE-2021-40482	Informazioaren hedapen erako ahultasuna Microsoft SharePoint Server-en	Garrantzitsua
CVE-2021-40481	Kodearen urruneko exekuzio erako ahultasuna Microsoft Office Visio-n	Garrantzitsua
CVE-2021-40480	Kodearen urruneko exekuzio erako ahultasuna Microsoft Office Visio-n	Garrantzitsua
CVE-2021-40479	Kodearen urruneko exekuzio erako ahultasuna Microsoft Excelen	Garrantzitsua
CVE-2021-41331	Kodearen urruneko exekuzio erako ahultasuna Windows Media-ren audio deskodegailuan	Garrantzitsua

CVE-2021-40473	Kodearen urruneko exekuzio erako ahultasuna Microsoft Excelen	Garrantzitsua
CVE-2021-41332	Informazioaren hedapen erako ahultasuna Windowsen inpresio ilaran	Garrantzitsua
CVE-2021-41335	Pribilegioen igotze erako ahultasuna Windowsen kernel-ean	Garrantzitsua
CVE-2021-41363	Intune-ren administrazio luzapenaren segurtasun ezaugarriaren gabezia erako ahultasuna	Garrantzitsua
CVE-2021-41357	Pribilegioen igotze erako ahultasuna Win32k-n	Garrantzitsua
CVE-2021-41354	Guneen artean komandoen sekuentzia erako ahultasuna Microsoft Dynamics 365-en (lokala)	Garrantzitsua
CVE-2021-41353	Ordezpen erako ahultasuna microsoft dynamics 365-en (lokala)	Garrantzitsua
CVE-2021-41352	Informazioaren hedapen erako ahultasuna SCOM-en	Garrantzitsua
CVE-2021-41347	Pribilegioen igotze erako ahultasuna Windowsen AppX-en Inplementazio zerbitzuan	Garrantzitsua
CVE-2021-41346	Kontsolako leihoaren host-aren segurtasun ezaugarriaren gabezia erako ahultasuna	Garrantzitsua
CVE-2021-41345	Pribilegioen igotze erako ahultasuna storage Spaces Controller-en	Garrantzitsua
CVE-2021-41343	Windowsen FAT fitxategi sistema azkarraren kontrolatzailearen informazioaren hedatze erako ahultasuna	Garrantzitsua
CVE-2021-41342	Kodearen urruneko exekuzio erako ahultasuna Windowsen MSHTML plataforman	Garrantzitsua

CVE-2021-41340	Kodearen urruneko exekuzio erako ahultasuna Windowsen grafikoen osagaian	Garrantzitsua
CVE-2021-41339	Pribilegioen igotze erako ahultasuna Microsoften DwM-ren liburutegi nagusian	Garrantzitsua
CVE-2021-41338	Windows AppContainer-en Firewall-aren segurtasun arauen ezaugarriaren gabezia erako ahultasuna	Garrantzitsua
CVE-2021-41337	Active Directory-ren segurtasun ezaugarriaren gabezia erako ahultasuna	Garrantzitsua
CVE-2021-41336	Informazioaren hedapen erako ahultasuna Windowsen kernel-ean	Garrantzitsua
CVE-2021-41334	Pribilegioen igotze erako ahultasuna Windows Desktop Bridge-n	Garrantzitsua
CVE-2021-40472	Informazioaren hedapen erako ahultasuna Microsoft Excelen	Garrantzitsua
CVE-2021-40474	Kodearen urruneko exekuzio erako ahultasuna Microsoft Excelen	Garrantzitsua
CVE-2021-40470	Pribilegioen igotze erako ahultasuna DirectX grafikoen kernel-ean	Garrantzitsua
CVE-2021-40471	Kodearen urruneko exekuzio erako ahultasuna Microsoft Excelen	Garrantzitsua
CVE-2021-41348	Pribilegioen igotze erako ahultasuna Microsoft Exchange Server-en	Garrantzitsua
CVE-2021-41344	Kodearen urruneko exekuzio erako ahultasuna Microsoft SharePoint Server-en	Garrantzitsua
CVE-2021-40478	Pribilegioen igotze erako ahultasuna storage Spaces Controller-en	Garrantzitsua
CVE-2021-40477	Pribilegioen igotze erako	Garrantzitsua

	ahultasuna Windowsen gertaeren segimenduan	
CVE-2021-40476	Pribilegioen igotze erako ahultasuna Windows AppContainer-en	Garrantzitsua
CVE-2021-40475	Informazioaren hedatze erako ahultasuna Windowsen Mini Filter Files kontrolatzailean	Garrantzitsua
CVE-2021-40457	Guneen artean komandoen sekuentzia erako ahultasuna Microsoft Dynamics 365 Customer Engagement-en	Garrantzitsua
CVE-2021-40456	Segurtasun ezaugarriaren gabezia erako ahultasuna Windows AD FS-n	Garrantzitsua
CVE-2021-40455	Ordezpen erako ahultasuna windows installer-en	Garrantzitsua
CVE-2021-40454	Aberastutako testuaren edizioaren kontrolaren informazioaren hedapen erako ahultasuna	Garrantzitsua
CVE-2021-40449	Pribilegioen igotze erako ahultasuna Win32k-n	Garrantzitsua
CVE-2021-40443	Pribilegioen igotze erako ahultasuna Windowsen erregistro komuneko fitxategien sistemaren kontrolatzailean	Garrantzitsua
CVE-2021-36970	Windowsen inpresio ilararen ordezpen erako ahultasuna	Garrantzitsua
CVE-2021-36953	Tcp/IP zerbitzuaren ukapen erako ahultasuna Windows-en	Garrantzitsua
CVE-2021-41355	Informazioaren hedapen erako ahultasuna .NET Core eta Visual Studio-n	Garrantzitsua
CVE-2021-41361	Active Directory-ren federazio zerbitzariaren identitatearen ordezpen erako ahultasuna	Garrantzitsua
CVE-2021-41350	Ordezpen erako ahultasuna microsoft exchange server-en	Garrantzitsua

CVE-2021-3449	OpenSSL: CVE-2021-3449 Deref erakuslearen null, signature algorithms-en prozesamenduan	Garrantzitsua
CVE-2021-40469	Kodearen urruneko exekuzio erako ahultasuna Windows DNS Server-en	Garrantzitsua
CVE-2021-40468	Pribilegioen igotze erako ahultasuna Windowsen erregistro komuneko fitxategien sistemaren kontrolatzailean	Garrantzitsua
CVE-2021-40467	Pribilegioen igotze erako ahultasuna Windowsen erregistro komuneko fitxategien sistemaren kontrolatzailean	Garrantzitsua
CVE-2021-40466	Pribilegioen igotze erako ahultasuna Windowsen erregistro komuneko fitxategien sistemaren kontrolatzailean	Garrantzitsua
CVE-2021-3450	OpenSSL: CA CVE-2021-3450 ziurtagirien egiaztapenaren gabezi erako ahultasuna X509_V_FLAG_X509_STRICT-ekin	Garrantzitsua
CVE-2021-40464	Pribilegioen igotze erako ahultasuna Windowsen erabilpen partekatu hurbilean	Garrantzitsua
CVE-2021-40463	Zerbitzuaren ukapen erako ahultasuna Windows NAT-en	Garrantzitsua
CVE-2021-40465	Kodearen urruneko exekuzio erako ahultasuna Windowsen testu konfigurazioan	Garrantzitsua
CVE-2021-40460	Windowsen urruneko prozeduretarako deien exekuzio denboran segurtasun ezaugarriaren gabezia erako ahultasuna	Garrantzitsua
CVE-2021-40450	Pribilegioen igotze erako ahultasuna Win32k-n	Garrantzitsua
CVE-2021-38663	Windowsen exFAT fitxategi sistemaren informazioaren hedatze erako ahultasuna	Garrantzitsua

CVE-2021-38662	Windowsen FAT fitxategi sistema azkarraren kontrolatzailearen informazioaren hedatze erako ahultasuna	Garrantzitsua
CVE-2021-26427	Urruneko kodearen exekuzio erako ahultasuna Microsoft Exchange Server-en	Garrantzitsua
CVE-2020-1971	OpenSSL: CVE-2020-1971 EDIPARTYNAME NULL erakuslearen deserreferentzia	Garrantzitsua
CVE-2021-40462	Kodearen urruneko exekuzio erako ahultasuna Windows Media Foundation-en Dolby Digital Atmos Decoders-en	Garrantzitsua
CVE-2021-40483	Ordezpen erako ahultasuna Microsoft Sharepoint server-en	**Baxua**
CVE-2021-37979	Chromium: CVE-2021-37979 Pilaren bufferraren gainezkatzea WebRTC-en	Kalifikaziorik gabe
CVE-2021-37974	Chromium: CVE-2021-37974 Doakoaren ondoreneko erabilpena nabigazio seguruan	Kalifikaziorik gabe
CVE-2021-37975	Chromium: CVE-2021-37975 Askatu ondoreneko erabilpena V8-n	Kalifikaziorik gabe
CVE-2021-37976	Chromium: CVE-2021-37976 Informazioaren ihesa nukleoan	Kalifikaziorik gabe
CVE-2021-37977	Chromium: CVE-2021-37977 Askatu ondoreneko erabilpena zaborra biltzean	Kalifikaziorik gabe
CVE-2021-37978	Chromium: CVE-2021-37978 Pilaren bufferraren gainezkatzea blink-en	Kalifikaziorik gabe
CVE-2021-37980	Chromium: CVE-2021-37980 Sandbox-en inplementazio desegokia	Kalifikaziorik gabe

4. ARINTZEA / KONPONBIDEA

Ahultasunak konpontzeko Microsoftek dagozkien segurtasun eguneraketak argitaratu ditu. Hil honetako argitalpenari buruzko oharrak eta eguneraketa gida berrikustea gomendatzen da.

Ohikoa den moduan, ahultasun hauek eta beste batzuk prebenitzeko BCSCk gomendatzen du gure sistemak eta aplikazioak azken bertsiora eguneratuta izatea beti.

5. ERREFERENTZIA OSAGARRIAK

- October 2021 Security Updates
- Security Update Guide - Microsoft
- Zero Day Initiative - The October 2021 Security Update Review

Gertakarien jakinarazpena

Zibersegurtasun gertakariren bat aurkitu baduzu jakinaraz iezaguzu, horrela beharrezkoak diren neurriak hartuko ditugu zabal ez dadin.

900 104 891

arazoak@bcsc.eus

Zibersegurtasun katalogoa

Zure zibersegurtasunarekin edo zure enpresarenarekin laguntza behar duzu?